物联网表箱智能网关的安全威胁与防护策略
——评《智能电网信息安全风险与防范研究》

随着智能电网建设的不断深入,物联网技术在电力行业的应用日益广泛。物联网表箱智能网关作为智能电网的重要组成部分,扮演着数据采集、传输和管理的关键角色。然而,随着物联网技术的普及,其面临的安全威胁也日益增多。

智能电网作为国家关键基础设施,其信息安全直接关系到国家安全、经济发展和社会稳定。笔者在开展国网山西省电力公司科技项目(项目编号:202406)过程中,阅读了《智能电网信息安全风险与防范研究》一书,探索了智能电网信息安全的新路径和防护体系。全书共分为6章,第1章介绍了智能电网的基本概念和特点、用电服务和发展现状;第2章论述了智能电网的系统架构和其中的有线通信及无线通信;第3章讲述了智能电网信息安全的内容并进行实例分析,论证了信息安全在智能电网中的重要性;第4章阐述了智能电网存在的信息安全危机,如拒绝服务攻击、勒索病毒攻击、供应链攻击及数据与隐私安全威胁;第5章分享了智能电网信息安全的防护措施;第6章描述了智能电网信息安全的发展新路径。

书名:智能电网信息安全风险与防范研究
作者:肖鹏
出版社:四川科学技术出版社
ISBN:9787572712395
出版时间:2024年1月
定价:58元

作者指出,智能电网信息安全至关重要,信息安全是智能电网建设和发展的重要前提。智能电网面临物联设备安全隐患、控制系统安全漏洞和数据安全与信息泄漏等多重信息安全威胁,需构建完善的信息安全防护体系来应对。作者强调,要建立智能电网网络安全应急响应机制及时应对可能发生的信息安全事件。同时,通过应急演练和培训,提高应对信息安全事件的能力和效率。

笔者认为,物联网表箱智能网关的安全性直接关系到电网的稳定运行和用户的隐私安全,必须高度重视物联网表箱智能网关的安全威胁,并采取有效的防护策略。目前,物联网表箱智能网关受到的安全威胁主要分为:①设备入侵与控制。物联网表箱智能网关可能因存在弱密码、漏洞和不安全配置等安全问题,而面临被攻击者入侵和控制的风险。一旦攻击者成功入侵设备,就可获取对电网的远程控制权限,进而实施恶意操作,如篡改用电数据、破坏电网稳定运行等。②数据泄漏与滥用。智能网关采集和传输数据包含用户的用电习惯、隐私信息等敏感数据。这些数据在传输、存储和处理过程中,如果未经妥善保护,可能面临泄漏和滥用的风险。一旦数据泄漏,将严重威胁用户隐私和电网安全。③网络攻击。物联网表箱智能网关连接到互联网,使其面临来自全球各地的网络攻击风险。常见的网络攻击手段包括分布式拒绝服务(DDoS)攻击、恶意软件和网络钓鱼等。这些攻击可能导致设备瘫痪、数据丢失或泄漏等严重后果。④无线通信安全威胁。物联网表箱智能网关通常使用无线通信技术与外界进行数据传输。然而,无线通信的安全性相对较弱,容易受到黑客攻击。攻击者通过破解无线通信协议、监听无线信号等手段,入侵智能网关系统,窃取或篡改数据。针对以上几类威胁,笔者认为,可采取相应的防护策略来应对。首先,加强设备安全设计与加密技术。物联网表箱智能网关制造商应加强设备的安全设计,包括硬件和软件层面的安全防护;同时,采用先进的加密技术,确保数据传输过程中机密性和完整性。其次,实施数据加密与备份策略。为保护物联网表箱智能网关采集和传输数据的安全,应实施数据加密和备份策略。通过加密技术,确保数据在传输过程中的机密性。此外,建立数据备份机制,防止数据丢失或损坏。然后,建立防火墙与入侵检测系统。物联网表箱智能网关应建立防火墙和入侵检测系统,以防范网络攻击。防火墙可阻止未经授权的访问和数据传输;入侵检测系统则可实时监测网络流量和异常行为,及时发现并应对网络攻击,而且还应定期更新和升级防火墙和入侵检测系统,确保其能够应对最新的网络威胁。再次,加强无线通信安全防护。针对物联网表箱智能网关的无线通信安全威胁,应采取加密通信、网络隔离和物理隔离等措施,通过加密无线通信协议,确保数据传输过程中的安全性。最后,提升用户安全意识与加强宣传。应加强宣传提升用户物联网表箱智能网关的安全意识,了解设备的安全风险和防范措施。通过提升用户的安全意识,共同维护物联网表箱智能网关的安全稳定。

在未来的智能电网建设中,应继续加强物联网技术的研发和应用,同时,注重安全技术的创新和提升。通过不断完善物联网表箱智能网关的安全防护体系,确保智能电网的安全稳定运行,为人们的生活和社会生产提供更加便捷、高效、安全的电力服务。

(赵强/国网晋中供电公司/高级经济师;李峰/国网晋中供电公司/高级工程师)